



**Homeland
Security**

Office of Inspector General
Evaluation of DHS' Security Program for Its Intelligence Systems
OIG-04-34

The E-Government Act (Public Law 107-347) passed by the 107th Congress and signed into law by the President on December 17, 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide security program. The agency's security program should provide security for the information and the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

The OIG performed an independent evaluation of DHS' security program for its intelligence systems as required by FISMA. The overall objective of this evaluation was to identify whether DHS' information security program and practices for its intelligence systems were adequate and effective in protecting the information from unauthorized access, use, disclosure, disruption, modification, or destruction. We reviewed five systems for compliance with FISMA and the Director of Central Intelligence Directive 6/3. We also performed vulnerability tests of security controls for these five systems. Furthermore, we evaluated DHS' Plan of Action and Milestones process for its intelligence systems and assessed DHS' security training program.

This review was conducted between April 2004 and July 2004. This report represents a baseline evaluation of DHS' intelligence program according to the Federal Information Security Management Act. We are posting only this summary on the OIG website because of a concern that information the report contains is sensitive and should not, consequently, be widely disseminated.